STM JOURNALS

Journal of
Mobile Computing, Communications & Mobile Networks

ISSN: 2349-901X
Volume 12, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoMCCMN

https://journals.stmjournals.com/jomccmn

Research JoMCCMN

Arduino Based Intelligent Building Security System

Vaishnavi Ramesh Veer*, Anjali Manik Girme, Shivani Ashok Lekawale, Dhanashri Adinath Pansare

Abstract

Intelligent Buildings are widely recognized as a forward-thinking solution for the future of architecture and urban development. Their successful implementation relies heavily on strategic planning that begins in the early stages of design. While this approach is somewhat aligned with current trends in green building projects, Intelligent Buildings go a step further by incorporating advanced technologies to improve functionality, efficiency, and the overall quality of indoor and outdoor spaces. These buildings typically feature integrated water management systems, sustainable construction materials, and energy-efficient layouts. Additional characteristics include thoughtful building orientation, incorporation of vegetation, and the use of smart systems that adapt to occupant needs. Despite their numerous advantages such as reducing operational staff requirements, enhancing tenant comfort, and lowering environmental impact, many of these benefits remain underappreciated or overlooked. One of the key reasons for the slow adoption of intelligent building technologies is the general lack of awareness, understanding, and confidence in their capabilities. Bridging this knowledge gap is essential for wider acceptance and implementation.

Keywords: Arduino building security system, RFID, Internet of Things (IoT), technology, GSM

INTRODUCTION

As technology continues to advance rapidly, security systems for homes and buildings have become essential for ensuring both safety and convenience for occupants. This Arduino-powered smart security system for homes and buildings incorporates several sophisticated features to meet these demands. Through the use of automation and live monitoring, it creates a secure and energy-conscious environment. An RFID-based access control system ensures that only authorized individuals, such as residents, can enter the premises, offering a modern alternative to conventional security methods.

In addition, the use of motion-sensor lighting in parking areas boosts safety while reducing energy consumption by activating lights only when movement from people or vehicles is detected. The system is also equipped with an MQ3 gas sensor for fire detection, which sends instant alerts via a GSM module when smoke or gas is detected, allowing residents to respond quickly in emergency situations and reduce possible damage.

Security is further strengthened with a keypad-enabled locking system for doors and lockers, allowing users to set custom passwords for controlled access. Altogether, this system blends advanced automation with reliable security features, providing a smart and efficient solution for modern buildings. At its core, the Arduino microcontroller coordinates all the connected technologies, including RFID tag readers, motion detectors like PIR or ultrasonic sensors, the MQ3 sensor, and

***Author for Correspondence**
Vaishnavi Ramesh Veer
E-mail: veervaishnavi78@gmail.com

Student, Department of Electronics and Telecommunications Engineering, Rajgad Dnyanpeeth Technical Campus, Dhangawadi, Tal. Bhor, Pune, Maharashtra, India

Received Date: April 05, 2025
Accepted Date: May 08, 2025
Published Date: June 18, 2025

Citation: Vaishnavi Ramesh Veer, Anjali Manik Girme, Shivani Ashok Lekawale, Dhanashri Adinath Pansare. Arduino Based Intelligent Building Security System. Journal of Mobile Computing, Communications & Mobile Networks. 2025; 12(2): 28–39p.

GSM communications. This integration ensures seamless operation, energy efficiency, and responsive protection tailored for smart living environments.

OBJECTIVE

The main purpose of the Arduino-powered smart home or building security system is to provide a safe, automated, and easy-to-use environment for its residents. A key objective is to prevent unauthorized entry by using RFID technology to control gate access, allowing only approved individuals to enter. Additionally, the system promotes energy conservation by using motion sensors in parking zones, so lights are only turned on when people or vehicles are present, helping to avoid wasting electricity. Another objective is to improve safety measures by incorporating an MQ3 sensor for fire or gas detection, instantly alerting users via GSM communication in case of emergencies. The system also focuses on enhancing the security of home doors and lockers by implementing a password-protected keypad system that permits only authorized users to obtain access. Additionally, it aims to offer a smooth transition between several automation and security functions into a single, integrated device. ensuring the system is both easy to manage and reliable. The goal is to create a real-time response system that guarantees timely action in emergency circumstances, lowering possible risks or damages. This project also seeks to utilize cost-effective and readily available components to enable a larger spectrum of consumers to utilize the smart security system. Overall, the objectives include enhancing security, improving energy efficiency, ensuring quick response to emergencies, and providing a customizable, user-centric solution suitable for modern smart buildings.

LITERATURE SURVEY

Design and Implementation of an Arduino Based Smart Home by Okorie *et al*.: The design and implementation of an affordable smart home that can be operated by an Android phone are presented in this study. This framework is designed to assist and accommodate the needs of elderly and disabled individuals within their homes. Additionally, integrating a smart home system aims to improve the overall comfort and wellbeing of the household. The system operates using analog sensors paired with a wireless Bluetooth connection, enabling smartphones to control it remotely. Rather than replacing existing electrical switches, the design introduces a safer method of managing them by utilizing low-voltage technology [1].

The article by Valov and Valova explores a home automation system built around the Raspberry Pi. It details how this compact computer works with various sensors to collect data. The Raspberry Pi serves as the central hub, running a software platform that not only processes and organizes the data but also manages different automation settings, controls connected household devices, and analyzes the gathered information [2].

Gate security systems rely on authentication techniques to control the hardware that either permits or blocks access to secured locations. The criteria for allowing user entry vary depending on the specific context. Despite the growing importance of these systems, there is a lack of standardized design recommendations. Much of the existing research concentrates on developing systems based on particular authentication methods, but does not offer broader design guidelines. This review adheres to the PRISMA framework to systematically examine recent studies on smart gate technologies. It evaluates research published from 2016 to 2023 to highlight key system components and authentication methods [3].

The study by Waheb *et al.* focuses on developing a smart home system powered by the Internet of Things (IoT) [4]. This system enables users to control and monitor home appliances through internet-connected automation. Traditional home automation setups often face issues such as high expense, poor wireless coverage, and complex user interfaces. To address these problems, the researchers propose an affordable IoT-based solution that supports both local and remote control, featuring a user-friendly design compatible with laptops and smartphones. With the rapid evolution of communication technologies, smart home automation has become an increasingly popular area of interest.

A smart home automation system based on Arduino microcontrollers was developed by Gota *et al.* [5]. This system enables home monitoring, control, and automation through the use of Internet of Things (IoT) technologies. Home automation represents an exciting advancement for tech enthusiasts, offering the ability to manage various household systems with ease. It also serves a valuable purpose for individuals with disabilities, allowing them to perform tasks such as locking doors, adjusting temperature, and monitoring ventilation via desktop applications or smartphones.

The study showcases a scaled-down model of a smart home, where LEDs are programmed to turn on and off in sequence or simultaneously. The setup includes actuators with a rotational range from 0 to 180°, which are used to open and close windows and doors, and can function as a remote-controlled door lock through a web-based interface.

EXISTING SYSTEM

The existing systems for home and building security often rely on traditional methods like manual locks, basic alarm systems, and standalone security cameras, which have significant limitations in terms of automation, accessibility, and real-time responsiveness [6–9]. These conventional systems typically lack integration, making it difficult to provide a cohesive security solution that can automate multiple functions simultaneously. For example, manually operated gates and locks require physical interaction, which can be inconvenient and insecure, as keys can be easily lost or duplicated.

Similarly, basic lighting systems in parking areas often stay on continuously, leading to unnecessary energy consumption and increased utility costs. Existing fire detection systems may trigger alarms, but they often fail to send timely alerts to the user when they are away from the premises, reducing the effectiveness of early intervention. Moreover, traditional locker or door lock systems with standard keys or outdated digital keypads are vulnerable to tampering and unauthorized access. These drawbacks indicate the need for a more advanced, automated security solution that integrates RFID access, motion-activated lighting, real-time fire alerts via GSM, and secure keypad-based systems, as proposed in the Arduino-based smart building security project [10–13].

Architecture of Existing System

The architecture of the existing system is based on Arduino, as illustrated in Figure 1.

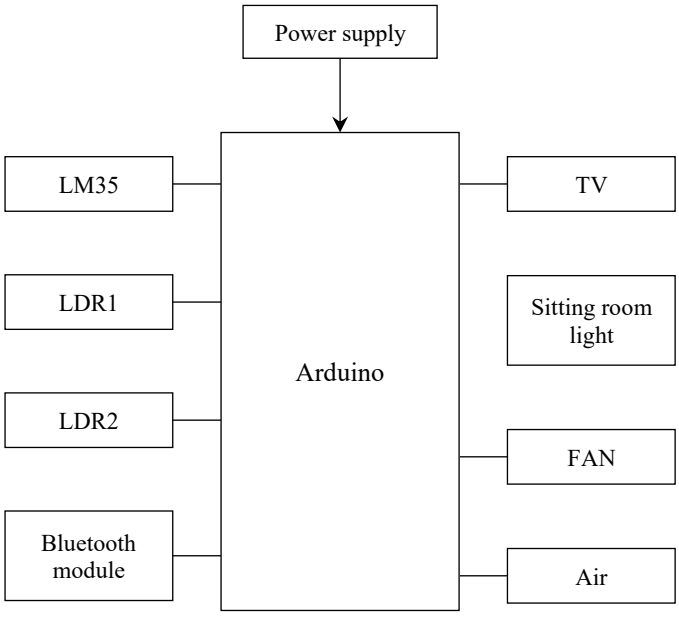

Figure 1. Architecture of existing system.

Limitations of Existing System

- *Lack of automation:* Traditional security systems rely heavily on manual operation, such as physically opening gates or locks, which can be inconvenient and time-consuming. Automated solutions are limited, making security management less efficient.
- *Fragmented solutions:* Most existing systems are standalone, such as separate alarm systems, cameras, or locks, which do not integrate well. This fragmentation makes it difficult to automate and manage multiple security aspects simultaneously, reducing overall system effectiveness.
- *Manual locks and key vulnerabilities:* Physical keys for doors and lockers can be lost, stolen, or duplicated, leading to potential unauthorized access. Additionally, key-based systems are prone to wear and tear over time, compromising security.
- *Energy inefficiency:* Traditional lighting systems, especially in parking areas, often remain on for long periods, even when not needed, resulting in significant energy wastage and higher utility costs.
- *Delayed fire alerts:* Conventional fire detection systems, while capable of triggering alarms, often lack the ability to notify the homeowner when they are away. This reduces the effectiveness of early intervention, which is critical in mitigating fire damage.
- *Insecure keypad systems:* Basic digital keypad locks used in some home security systems are often outdated, making them vulnerable to tampering or hacking. These systems provide minimal protection against modern security threats.
- *Inaccessibility in remote scenarios:* Traditional systems often fail to provide real-time notifications to the homeowner when they are off-site, leaving the home vulnerable when immediate action is required.
- *Limited customization:* Many traditional security systems offer limited user customization options, such as setting personal access codes or configuring alert mechanisms, restricting users' ability to tailor security measures to their specific needs.

PROPOSED SYSTEM

The Arduino-powered smart home or building security system being proposed is designed to bring together several automated features to boost both safety and ease of use for residents [14–17]. A standout element of this setup is the RFID-controlled gate system, which restricts entry to only those who are authorized, typically the homeowners or flat occupants. When the system detects an approved RFID tag, the gate opens automatically, allowing secure and hands-free entry. This ensures that unauthorized individuals are kept out, enhancing the building's overall safety.

In the parking zone, motion sensors are installed to detect the presence of people or vehicles. As soon as any movement is identified, the lighting system turns on for a set amount of time to improve visibility and ensure safety. Once the area becomes inactive, the lights shut off automatically, helping to conserve electricity and lower energy bills, making the system not just secure but energy-conscious as well [18–20].

Another vital component is the fire safety feature, which uses an MQ3 sensor to monitor for smoke or gas leaks. If a fire or leak is detected, the system immediately sends a warning to the homeowner via a GSM module, enabling quick response and potentially preventing serious damage. This immediate alert system plays a key role in protecting both lives and property.

For added security, especially for interior doors and lockers, the system includes keypad-based locks. Residents can set a custom code to access these areas, ensuring that only those with the correct password can open them. This adds another layer of protection for personal belongings and valuable items.

Altogether, this integrated system, combining RFID access, motion-sensing lights, fire detection, and keypad locks, offers a well-rounded, intelligent solution for modern residential security and energy management.

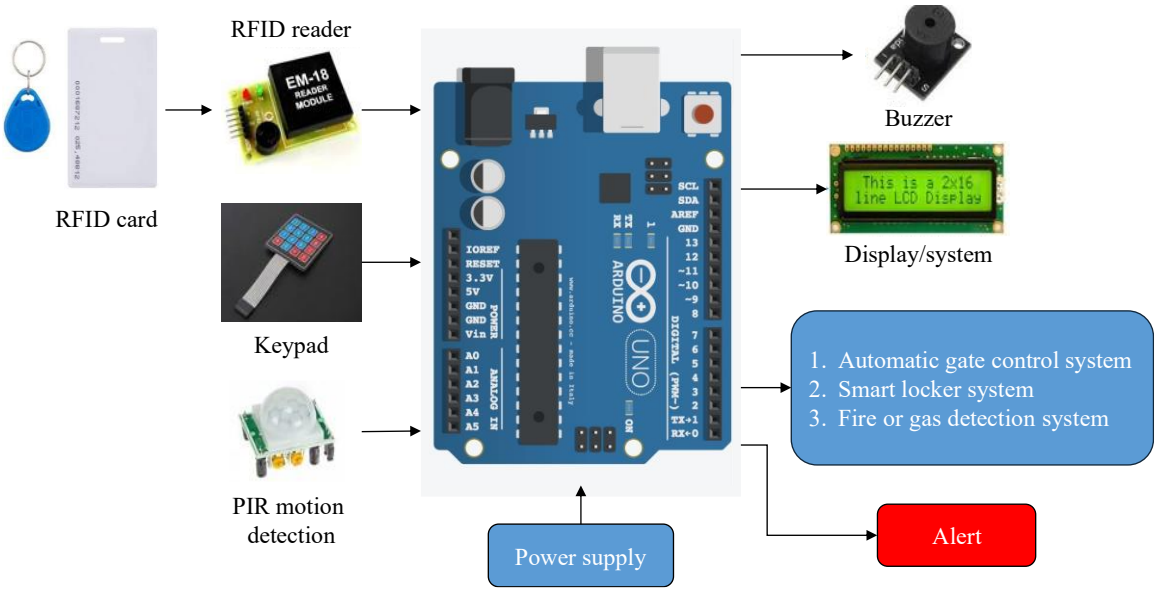

Figure 2. Architecture of proposed work.

The ultimate goal of this Arduino-driven security solution is to significantly improve how safe, convenient, and energy-efficient residential spaces can be. The RFID gate ensures controlled access, allowing only authorized individuals to enter, while motion sensors in parking areas reduce wasted electricity by activating lights only when needed. The fire alert system delivers immediate warnings via GSM, helping prevent major losses in case of emergencies. Additionally, keypad-locked access points protect sensitive areas within the home. By blending multiple safety technologies into one cohesive setup, the system promises a smarter, safer, and more efficient living experience for today's homeowners (Figure 2).

System Requirement Specification

This section outlines the essential requirements for implementing the Arduino-based smart home or building security system. The system necessitates both hardware and software components to function optimally. On the hardware side, an i3 processor or higher, with a speed of 2.0 GHz or higher, 8 GB of RAM, and 120 GB SSD storage is required. Key hardware components include the Arduino UNO, RFID reader, RFID tags, MQ3 sensor, PIR sensor, GSM module, and other essential components like keypads, cables, and connectors. On the software side, Windows 10 is needed for the operating system, and Android Studio is required for platform development, with a database to handle sensor data efficiently. The requirements analysis phase further identifies the necessary hardware, software, database, and interfaces to ensure the smooth integration and functioning of the system.

Hardware Resource Required

- Processor : i3 Or Higher
- Processor speed : 2.0 GHz or Higher
- RAM : 8 GB
- Disk Space : 120 GB SSD.
- Arduino UNO, RFID reader, RFID card, Keypad, MQ3, PIR, GSM, Power Cable, Cable, Wire, etc.

Software Resource Required

- Operating system : Windows 10
- Platform : Android Studio
- Database : Sensor Data

Required Analysis

In this step of waterfall, we identify what are the various requirements for our project such as software and hardware required, database, and interfaces.

METHODOLOGY

RFID-Based Gate Control

- *Component:* RFID Reader, RFID Tags, Servo Motor.
- *Functionality:* Each homeowner or flat owner is assigned an RFID tag.
- The system verifies the user when the RFID reader at the gate scans the RFID tag.
- If authenticated, the gate opens automatically using a servo motor.
- Once the vehicle or person enters, the gate closes after a short delay, ensuring security and smooth operation.

Parking Area Lighting Control

- *Component:* PIR (Passive Infrared) Motion Sensor, Relay Module, Lighting System.
- *Functionality:* PIR sensors are placed at strategic locations in the parking area.
- When the system detects movement (either a human or vehicle), the relay module is triggered, turning the lights on.
- Lights remain on for a predefined time (e.g., 30 sec) and automatically turn off when no further motion is detected, conserving energy.

Fire Detection and Alert System

- *Component:* MQ-3 Gas Sensor, GSM Module.
- *Functionality:* The MQ-3 sensor continuously monitors the environment for smoke or gas leakage (potential fire hazards).
- When the sensor identifies unusual readings, the Arduino activates the GSM module to send a notification to the homeowner's phone.
- This ensures immediate notification, allowing the homeowner to take necessary precautions or contact emergency services.

Keypad-Based Door Lock/Locker System

- *Component:* Keypad, Solenoid Lock, Arduino.
- *Functionality:* A digital keypad is installed at the home door or locker, allowing users to enter a custom-set password.
- The Arduino verifies the entered password against the stored one.
- If the password matches, the solenoid lock disengages, granting access to the home or locker.
- If the password is wrong, access will be blocked, and optional alarms can be added for extra security.

System Integration and Real-Time Control

- *Component:* Arduino Microcontroller.
- *Functionality:* The Arduino microcontroller acts as the central controller, managing inputs from the RFID reader, PIR sensor, MQ-3 sensor, and keypad.
- It processes the data and sends signals to the respective actuators (servo motor for gate, lights for parking, GSM for alerts, solenoid lock for lockers).
- The system operates in real-time, ensuring fast and efficient responses to events.

Energy Efficiency and Power Management

- *Component:* Power Supply, Relay, Timer Logic.
- *Functionality:* The system is designed to minimize energy consumption by automatically controlling lighting in the parking area based on motion detection.

- The RFID, keypad, and fire detection systems are low-power components that only activate the necessary modules when required, ensuring efficient energy usage.

Modules

RFID-Based Gate Access Control

The first module of the system involves RFID-based access control at the gate. This module is responsible for managing the entry and exit of residents or authorized individuals. Each flat or house owner is provided with an RFID tag that, when scanned at the gate, automatically opens the entrance. This ensures secure and hassle-free access, allowing only those with valid RFID tags to enter. Unauthorized access attempts will be prevented, enhancing the security of the building or residential area. This module can also log entry times for additional monitoring.

Motion Sensor-Based Parking Lighting

The second module focuses on energy-efficient lighting in parking areas. It uses motion sensors to sense the presence of people or vehicles. When movement is detected, the lights are automatically switched on for a preset duration, providing adequate illumination for safety and convenience. Once no further activity is detected, the lights are turned off to save energy. This automatic lighting system ensures that lights are only activated when necessary, thus reducing electricity consumption and operational costs.

Fire Detection and Alert System

The third module is the fire detection system, which uses an MQ3 sensor to monitor smoke and gas levels. If a fire or dangerous gas is detected, the system activates an alarm. This alert is transmitted to the building owner or security personnel via a GSM module. The instant alert mechanism ensures prompt action, allowing for faster responses to potential emergencies. This module is crucial for ensuring the safety of both residents and property, as it can prevent severe damage through early detection and notification.

Keypad-Based Locking System

The fourth module provides security for home doors or lockers through a keypad-based locking mechanism. Residents can set a personalized password to secure their doors or valuable storage areas, such as lockers. The system can only be accessed by those who have the correct password, ensuring that unauthorized users are kept out. This module provides an additional layer of security for personal belongings and critical areas within the home, ensuring that valuables are protected from theft or unauthorized use.

GSM Alert Communication

The final module handles communication with residents or security personnel through GSM technology. This module integrates with other systems, such as the fire detection module, to send immediate alerts when an emergency is detected. It can also be programmed to send notifications for other security breaches, such as unauthorized gate access attempts or incorrect password entries on the keypad lock. The GSM-based alert system ensures that residents are kept informed about potential security threats or emergencies in real time, even when they are away from the premises.

Hardware Used

In the proposed Arduino-based smart building or home security system, the following hardware components are used, each playing a crucial role in implementing the various security features.

Arduino Uno

This microcontroller board serves as the brain of the system, processing inputs from sensors and controlling the outputs based on programmed instructions, as illustrated in Figure 3. It is responsible for managing the RFID system, motion sensors, MQ3 gas sensor, and keypad inputs, while coordinating responses like opening gates, turning on lights, and sending alerts.

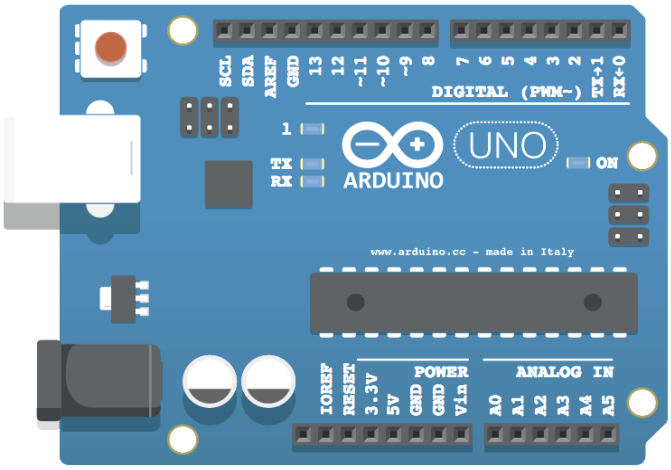

Figure 3. Arduino UNO.

Figure 4. EM18 RFID reader module.

Figure 5. RFID card.

Figure 6. PIR.

RFID Module

The RFID module is used for secure gate access control, as illustrated in Figure 4. It reads the RFID tags carried by authorized individuals (homeowners or flat owners). When a recognized RFID tag is detected, the Arduino triggers a signal to open the gate, granting access. This process guarantees that only authorized individuals can enter the premises, as illustrated in Figure 5.

Motion Sensor (PIR Sensor)

The Passive Infrared (PIR) sensor in the parking area detects the presence of people or vehicles, as illustrated in Figure 6. When it senses movement, it activates the lights to provide visibility and enhance safety. After a certain period of no movement, the lights automatically shut off to save energy.

MQ3 Gas Sensor

The MQ3 sensor is used for fire detection, as illustrated in Figure 7. It detects smoke or gas emissions that may indicate a fire or gas leak. Once a dangerous level is sensed, it sends an alert signal to the Arduino, which then triggers the GSM module to notify the user immediately via SMS, allowing for timely action.

GSM Module (SIM900)

This module is used to send real-time alerts to the homeowner in case of emergencies, such as a fire. The Arduino communicates with the GSM module to send an SMS alert containing details of the detected issue, enabling the homeowner to respond promptly, as illustrated in Figure 8.

Keypad (4×4 Matrix)

The keypad is used for secure access to the home door or lockers, as illustrated in Figure 9. It allows users to enter a preset password to unlock the system.

Figure 7. MQ3.

Figure 8. GSM.

Figure 9. Keypad.

The keypad sends input signals to the Arduino, which checks the entered password and, if correct, opens the lock. This adds an extra layer of security to lockers or doors.

Motor

The servo motor is used to control the physical opening and closing of the gate or door locks. When the Arduino receives the correct RFID signal or password input, it sends a signal to the servo motor to move, unlocking or locking the gate or door as required.

Relay Module

The relay module is employed to manage high-power devices like lights or gate motors. It acts as a switch that allows the Arduino to control these devices by turning them on or off based on input signals from sensors or the RFID system.

Buzzer

A buzzer may be used as an audible alarm system. It can provide alerts in the event of an unauthorized entry attempt or when the MQ3 sensor detects smoke or gas. The buzzer gives a real-time, attention grabbing alert to the occupants.

Power Supply (Battery/Adapter)

The system requires a stable power source to function. A regulated power supply, such as a 12 V adapter or battery, powers the Arduino and connected components, ensuring consistent operation across the system.

ADVANTAGES

- The suggested smart building and home security system, built on Arduino, provides a range of benefits.
- It improves security by granting access to the premises only to authorized individuals through RFID-enabled gate control, ensuring that entry is limited.
- The system improves energy efficiency by using motion sensors to activate lights only when human or vehicle movement is detected, saving power by turning them off when not needed.
- The fire detection feature using the MQ3 sensor ensures early detection of smoke or gas, with immediate alerts sent via GSM for prompt action, minimizing potential damage.
- The keypad lock system provides an extra level of security, allowing access to restricted areas such as lockers or doors only for those who have the correct password.
- The system's automation reduces manual intervention, providing convenience to users. Its real-time notification system allows for quick reactions to emergencies, improving overall safety.
- The customizable password feature for door and locker access allows for personal security preferences.
- By integrating multiple security features, the system offers comprehensive protection for both residents and their property.

- Additionally, it is scalable, allowing further integration of security enhancements, and cost-effective due to its reliance on Arduino, making it an ideal solution for modern smart homes.

DISADVANTAGES

- One of the main disadvantages of the proposed Arduino-based smart building or home security system is its reliance on external hardware components, such as RFID tags, motion sensors, and keypad systems, which may experience wear and tear over time, leading to potential failures or inaccuracies.
- For example, RFID tags can be misplaced or malfunction, restricting access for the rightful owner.
- Additionally, the motion sensors in the parking area may trigger false alarms due to non-human movements, such as animals or environmental factors like wind, resulting in unnecessary energy consumption.
- Another concern is that the system's GSM module depends on a stable cellular network, and in areas with weak signal coverage, critical fire alerts may be delayed or missed, potentially leading to delayed responses in emergency situations.
- Lastly, the keypad system for lockers might be vulnerable to password guessing or hacking if strong security measures, such as encryption, are not implemented.

APPLICATIONS

- *Residential buildings and apartments:* The system is ideal for gated communities, apartment complexes, or individual homes where security is a priority. The RFID-based gate access ensures that only authorized residents can enter, preventing unauthorized access. Additionally, the motion sensor-controlled lighting system in parking areas enhances safety for both pedestrians and vehicles, while conserving energy by turning off lights when no movement is detected.
- *Commercial complexes and offices:* In commercial buildings, the RFID system can regulate employee or authorized personnel access to restricted areas, while the motion-sensor lighting system can reduce energy consumption in parking lots and less-frequented areas. The fire detection system can be crucial in protecting office assets and ensuring timely evacuation during emergencies. Additionally, the keypad-based locker system can provide secure storage for important documents or valuables in offices.
- *Smart homes and automation:* For modern smart homes, this system can act as a comprehensive security solution. The RFID-based access, fire detection with GSM alerts, and secure keypad lockers can provide homeowners with peace of mind, knowing their home is automated and secure even when they are away.
- *Parking garages and public buildings:* The motion-detecting lights can be applied in parking garages or public buildings, where energy-saving features are essential. Coupled with the security features, this system can ensure that unauthorized vehicles or individuals do not gain access, providing added security for public infrastructure.

FUTURE SCOPE

The future scope of the Arduino-based smart building or home security system is expansive, allowing for numerous enhancements and integrations that could significantly improve its functionality and user experience. A possible advancement is the addition of sophisticated biometric authentication techniques, like fingerprint or facial recognition, alongside the current RFID and keypad systems, boosting security by guaranteeing that only approved individuals can enter restricted areas. Additionally, incorporating smart home technologies can enable the system to connect with other IoT devices, allowing for centralized control of various home appliances and systems through a single interface, such as a mobile app. This could include automated climate control, surveillance cameras with real-time video feeds, and remote access management for the security system. Moreover, leveraging machine learning algorithms could enable the system to learn from user behaviors, predicting and adapting to their needs while optimizing energy usage and security protocols. The addition of environmental sensors for monitoring air quality and temperature can further improve the living

conditions within the building, providing alerts for any abnormalities. Furthermore, establishing a cloud-based data storage solution could facilitate remote monitoring and management of the system, enabling users to receive alerts and control the system from anywhere in the world. Overall, the future scope encompasses a holistic approach to smart living, emphasizing security, efficiency, and user convenience while adapting to emerging technologies.

RESULT

In the results section, the outcome of integrating the various features of the Arduino-based smart security system is analyzed. The system aims to enhance security, energy efficiency, and safety in residential or commercial buildings. Through the use of RFID-based gate control, it ensures that only authorized personnel gain access to the premises. The motion sensor-based lighting system in parking areas reduces energy consumption by only activating lights when movement is detected. Fire detection using the MQ3 sensor offers immediate alerts, enabling quick action to minimize damage. The keypad locking system adds an extra layer of security for sensitive areas within the premises. Overall, the system operates efficiently, providing real-time alerts and ensuring optimal security and energy management, delivering the desired outcomes for modern smart living environments.

CONCLUSION

In summary, the Arduino-powered smart building or home security system presents a comprehensive solution for improving safety and comfort for residents. By incorporating features like RFID-based gate access, motion-triggered lighting, fire detection with an MQ3 sensor, and a keypad-locked system, this approach addresses several modern security requirements. The RFID system ensures that only authorized individuals can access the property, reducing the chances of unauthorized entry, while the motion sensors in the parking area provide targeted lighting that improves security without wasting power. The fire detection function is a vital safety element, offering instant alerts via the GSM module, which can significantly shorten emergency response times. Additionally, the keypad-locked locker system provides extra protection for personal items, giving users control and privacy over their possessions. Overall, this system not only focuses on enhancing user safety and convenience but also aligns with the growing trend of integrating smart technology into residential environments, making it a valuable solution for tackling today's security challenges.

REFERENCES

1. Okorie PU, Ibraim AA, Auwal D. Design and implementation of an arduino based smart home. In 2020 IEEE International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2020 Jun 26; 1–6.
2. Valov N, Valova I. Home automation system with Raspberry Pi. In 2020 IEEE 7th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE). 2020 Nov 12; 1–5.
3. Omotunde Habeeb, Ahmed Maryam. A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. Mesopotamian Journal of Cyber Security (MJCS). 2023; 2023: 115–133. 10.58496/MJCSC/2023/016.
4. Al-Areeqi Waheb, Kian Tee, Ramli Roshahliza, Zubir Siti, Zamrizaman Nurthaqifah, Balfaqih Mohammed, Shepelev Vladimir, Alharbi Soltan. Design and Fabrication of Smart Home With Internet of Things Enabled Automation System. IEEE Access. 2019; 7: 144059–144074. 10.1109/ACCESS.2019.2942846.
5. Gota DI, Puscasiu A, Fanca A, Miclea L, Valean H. Smart home automation system using Arduino microcontrollers. In 2020 IEEE International conference on automation, quality and testing, robotics (AQTR). 2020 May 21; 1–7.
6. Lartigue JW, McKinney C, Phelps R, Rhodes R, Rice AD, Ryder A. A tablet-controlled, mesh-network security system: An architecture for a secure, mesh network of security and automation systems using Arduino and Zigbee controllers and an android tablet application. In Proceedings of the 2014 ACM Southeast Conference. 2014 Mar 28; 1–4.

7. Fuzi MF, Ibrahim AF, Ismail MH, Ab Halim NS. HOME FADS: A dedicated fire alert detection system using ZigBee wireless network. In 2014 IEEE 5th control and system graduate research colloquium. 2014 Aug 11; 53–58.
8. Chowdhry D, Paranjape R, Laforge P. Smart home automation system for intrusion detection. In 2015 IEEE 14th Canadian workshop on information theory (CWIT). 2015 Jul 6; 75–78.
9. Anani W, Ouda A, Hamou A. A survey of wireless communications for IoT echo-systems. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). 2019 May 5; 1–6.
10. Yassein MB, Hmeidi I, Shatnawi F, Mardini W, Khamayseh Y. Smart home is not smart enough to protect you-protocols, challenges and open issues. Procedia Comput Sci. 2019 Jan 1; 160: 134–41.
11. Daissaoui A, Boulmakoul A, Karim L, Lbath A. IoT and big data analytics for smart buildings: A survey. Procedia Comput Sci. 2020 Jan 1; 170: 161–8.
12. Williams V, Immaculate J. Survey on Internet of Things based smart home. In 2019 IEEE International Conference on Intelligent Sustainable Systems (ICISS). 2019 Feb 21; 460–464.
13. Alaa M, Zaidan AA, Zaidan BB, Talal M, Kiah ML. A review of smart home applications based on Internet of Things. J Netw Comput Appl. 2017 Nov 1; 97: 48–65.
14. Asadullah M, Raza A. An overview of home automation systems. In 2016 IEEE 2nd international conference on robotics and artificial intelligence (ICRAI). 2016 Nov 1; 27–31.
15. Hasan M, Biswas P, Bilash MT, Dipto MA. Smart home systems: Overview and comparative analysis. In 2018 IEEE Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN). 2018 Nov 22; 264–268.
16. Karimi K, Krit S. Smart home-smartphone systems: Threats, security requirements and open research challenges. In 2019 IEEE International Conference of Computer Science and Renewable Energies (ICCSRE). 2019 Jul 22; 1–5.
17. Komninos N, Philippou E, Pitsillides A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Commun Surv Tutor. 2014 Apr 24; 16(4): 1933–54.
18. Lee C, Zappaterra L, Choi K, Choi HA. Securing smart home: Technologies, security challenges, and security requirements. In 2014 IEEE Conference on Communications and Network Security. 2014 Oct 29; 67–72.
19. Bugeja J, Jacobsson A, Davidsson P. On privacy and security challenges in smart connected homes. In 2016 IEEE European intelligence and security informatics conference (EISIC). 2016 Aug 17; 172–175.
20. Batalla JM, Vasilakos A, Gajewski M. Secure smart homes: Opportunities and challenges. ACM Comput Surv. 2017 Sep 26;50(5):1–32.

